

Question 1

Match the description to the type of firewall filtering. (Not all options are used.)

Stateful packet inspection: Prevents or allows access based on whether the traffic is in response to requests from internal hosts.

URL filtering: Prevents or allows access based on web addresses or keywords.

Application filtering: Prevents or allows access based on the port numbers used in the request.

Packet filtering: Prevents or allows access based on the IP or MAC addresses of the source and destination.

Question 2

Which firewall feature is used to ensure that packets coming into a network are legitimate responses to requests initiated from internal hosts?

- application filtering
- **stateful packet inspection**
- packet filtering
- URL filtering

Explanation:

Stateful packet inspection on a firewall checks that incoming packets are actually legitimate responses to requests originating from hosts inside the network.

Packet filtering can be used to permit or deny access to resources based on IP or MAC address.

Application filtering can permit or deny access based on port number.

URL filtering is used to permit or deny access based on URL or on keywords.

Question 3

What is the purpose of the network security authentication function?

- **to require users to prove who they are**
- to determine which resources a user can access
- to keep track of the actions of a user
- to provide challenge and response questions

Explanation: Authentication, authorization, and accounting are network services collectively known as AAA.

Authentication requires users to prove who they are.

Authorization determines which resources the user can access.

Accounting keeps track of the actions of the user.

Question 4

What feature of SSH makes it more secure than Telnet for a device management connection?

- confidentiality with IPsec
- stronger password requirement
- random one-time port connection
- **login information and data encryption**

Explanation: Secure Shell (SSH) is a protocol that provides a secure management connection to a remote device. SSH provides security by providing encryption for both authentication (username and password) and the transmitted data. Telnet is a protocol that uses unsecure plaintext transmission. SSH is assigned to TCP port 22 by default. Although this port can be changed in the SSH server configuration, the port is not dynamically changed. SSH does not use IPsec.

Question 5

A user is redesigning a network for a small company and wants to ensure security at a reasonable price. The user deploys a new application-aware firewall with intrusion detection capabilities on the ISP connection. The user installs a second firewall to separate the company network from the public network. Additionally, the user installs an IPS on the internal network of the company. What approach is the user implementing?

- attack based
- risk based
- structured
- **layered**

Explanation: Using different defenses at various points of the network creates a layered approach.

Question 6

Which attack involves a compromise of data that occurs between two end points?

- denial-of-service
- **man-in-the-middle attack**
- extraction of security parameters
- username enumeration

Explanation: Threat actors frequently attempt to access devices over the internet through communication protocols. Some of the most popular remote exploits are as follows:

- **Man-In-the-middle attack (MITM)** - The threat actor gets between devices in the system and intercepts all of the data being transmitted. This information could simply be collected or modified for a specific purpose and delivered to its original destination.
- **Eavesdropping attack** - When devices are being installed, the threat actor can intercept data such as security keys that are used by constrained devices to establish communications once they are up and running.
- **SQL injection (SQLi)** - Threat actors use a flaw in the Structured Query Language (SQL) application that allows them to have access to modify the data or gain administrative privileges.
- **Routing attack** - A threat actor could either place a rogue routing device on the network or modify routing packets to manipulate routers to send all packets to the chosen destination of the threat actor. The threat actor could then drop specific packets, known as selective forwarding, or drop all packets, known as a sinkhole attack.

Question 7

Match the type of information security threat to the scenario. (Not all options are used.)

Explanation:

After an intruder gains access to a network, common network threats are as follows:

- **Information theft** - obtaining trade secret documents illegally

- **Identity theft** - pretending to be someone else by using stolen personal information to apply for a credit card
- **Data loss or manipulation** - installing virus code to destroy surveillance recordings for certain days
- **Disruption of service** - preventing users from accessing a website by sending a large number of link requests in a short period.

Question 8

Identify the steps needed to configure a switch for SSH. The answer order does not matter. (Not all options are used.)

Create a local user - SSH configuration step

Generate RSA keys - SSH configuration step

Configure a domain name - SSH configuration step

Use the login local command - SSH configuration step

Use the transport input ssh command - SSH configuration step

Explanation: The **login** and **password cisco** commands are used with Telnet switch configuration, not SSH configuration.

Question 9

Match each weakness with an example. (Not all options are used.)

configuration weakness -- when implementing an access list on a router, a network engineer did not filter a type of malicious traffic

technological weakness -- a network engineer is examining the operating system of a network device for vulnerabilities

security policy weakness -- the network administrator did not fully consider the implications of unauthorized users accessing the network.

Question 10

What is the difference between a virus and a worm?

- Viruses self-replicate but worms do not.
- **Worms self-replicate but viruses do not.**
- Worms require a host file but viruses do not.
- Viruses hide in legitimate programs but worms do not.

Explanation: Worms are able to self-replicate and exploit vulnerabilities on computer networks without user participation.

Question 11

Which type of attack involves an adversary attempting to gather information about a network to identify vulnerabilities?

- **reconnaissance**
- DoS
- dictionary
- man-in-the-middle

Explanation: Reconnaissance is a type of attack where the intruder is looking for wireless network vulnerabilities.

Question 12

An employee complains that a Windows PC cannot connect to the Internet. A network technician issues the ipconfig command on the PC and is shown an IP address of 169.254.10.3. Which two conclusions can be drawn? (Choose two.)

- **The PC cannot contact a DHCP server.**
- The DNS server address is misconfigured.
- The default gateway address is not configured.
- **The PC is configured to obtain an IP address automatically.**
- The enterprise network is misconfigured for dynamic routing.

Explanation: When a Windows PC is configured to obtain an IP address automatically, the PC will try to obtain an IP address from a DHCP server. When the PC cannot contact a DHCP server, Windows will automatically assign an address belonging to the 169.254.0.0/16 range.

Question 13

Which command can an administrator issue on a Cisco router to send debug messages to the vty lines?

- **terminal monitor**
- logging console
- logging buffered

- logging synchronous

Explanation: Debug messages, like other IOS log messages, are sent to the console line by default. Sending these messages to the terminal lines requires the **terminal monitor** command.

Question 14

A network engineer is troubleshooting connectivity issues among interconnected Cisco routers and switches. Which command should the engineer use to find the IP address information, host name, and IOS version of neighboring network devices?

- show version
- show ip route
- show interfaces
- **show cdp neighbors detail**

Explanation: The **show cdp neighbors detail** command reveals much information about neighboring Cisco devices, including the IP address, the capabilities, host name, and IOS version. The **show interfaces** and **show version** commands display information about the local device.

Question 15

Which method is used to send a ping message specifying the source address for the ping?

- Issue the ping command from within interface configuration mode.
- **Issue the ping command without specifying a destination IP address.**
- Issue the ping command without extended commands.
- Issue the ping command after shutting down un-needed interfaces.

Explanation: By issuing the **ping** command without a destination IP address in privileged EXEC mode, the Cisco IOS enters extended ping mode. This allows the user to implement extended commands which include source IP address.

Question 16

By following a structured troubleshooting approach, a network administrator identified a network issue after a conversation with the user. What is the next step that the administrator should take?

- Verify full system functionality.
- Test the theory to determine cause.
- **Establish a theory of probable causes.**
- Establish a plan of action to resolve the issue.

Explanation: A structured network troubleshooting approach should include these steps in sequence:

1. Identify the problem.
2. Establish a theory of probable causes.
3. Test the theory to determine cause.
4. Establish a plan of action to resolve the issue.
5. Verify full system functionality and implement preventive measures.
6. Document findings, actions, and outcomes.

Question 17

Which command should be used on a Cisco router or switch to allow log messages to be displayed on remotely connected sessions using Telnet or SSH?

- debug all
- logging synchronous
- show running-config
- **terminal monitor**

Explanation: The terminal monitor command is very important to use when log messages appear. Log messages appear by default when a user is directly consoled into a Cisco device, but require the terminal monitor command to be entered when a user is accessing a network device remotely.

Question 18

What information about a Cisco router can be verified using the show version command?

- the routing protocol version that is enabled
- **the value of the configuration register**
- the operational status of serial interfaces
- the administrative distance used to reach networks

Explanation: The value of the configuration register can be verified with the **show version** command.

Question 19

Which statement is true about Cisco IOS ping indicators?

- '!' indicates that the ping was unsuccessful and that the device may have issues finding a DNS server.
- **'U' may indicate that a router along the path did not contain a route to the destination address and that the ping was unsuccessful.**
- '.' indicates that the ping was successful but the response time was longer than normal.
- A combination of '.' and '!' indicates that a router along the path did not have a route to the destination address and responded with an ICMP unreachable message.

Explanation: The most common indicators of a ping issued from the Cisco IOS are "!", ".", and "U". The "!" indicates that the ping completed successfully, verifying connectivity at Layer 3. The "." may indicate that a connectivity problem, routing problem, or device security issue exists along the path and that an ICMP destination unreachable message was not provided. The "U" indicates that a router along the path may not have had a route to the destination address, and that it responded with an ICMP unreachable message.

Question 20

Refer to the exhibit. An administrator is testing connectivity to a remote device with the IP address 10.1.1.1. What does the output of this command indicate?

```
Switch# ping 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
UUUUU
Success rate is 0 percent (0/5)
```


- Connectivity to the remote device was successful.
- **A router along the path did not have a route to the destination.**
- A ping packet is being blocked by a security device along the path.
- The connection timed out while waiting for a reply from the remote device.

Explanation: In the output of the ping command, an exclamation mark (!) indicates a response was successfully received, a period (.) indicates that the connection timed out while waiting for a reply, and the letter “U” indicates that a router along the path did not have a route to the destination and sent an ICMP destination unreachable message back to the source.

Question 21

What is an accurate description of redundancy?

- configuring a router with a complete MAC address database to ensure that all frames can be forwarded to the correct destination
- configuring a switch with proper security to ensure that all traffic forwarded through an interface is filtered
- designing a network to use multiple virtual devices to ensure that all traffic uses the best path through the internetwork
- **designing a network to use multiple paths between switches to ensure there is no single point of failure**

Explanation: Redundancy attempts to remove any single point of failure in a network by using multiple physically cabled paths between switches in the network.

Question 22

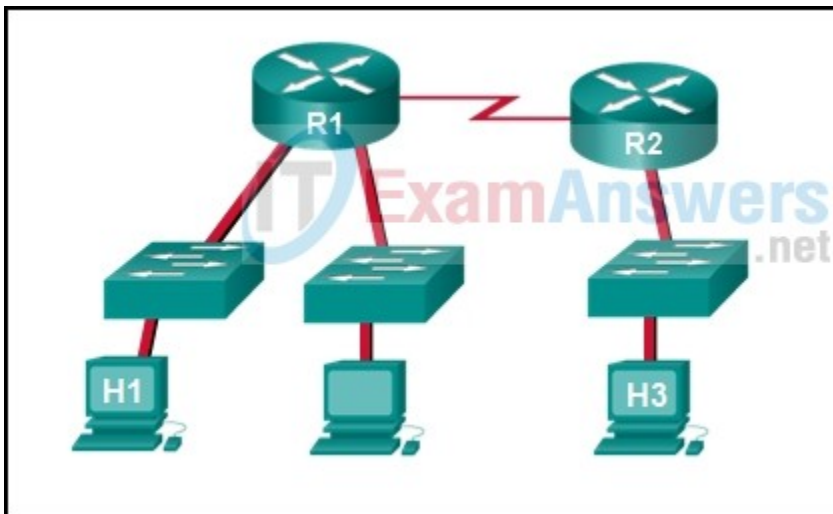
A network engineer is analyzing reports from a recently performed network baseline. Which situation would depict a possible latency issue?

- a change in the bandwidth according to the show interfaces output
- a next-hop timeout from a traceroute
- **an increase in host-to-host ping response times**
- a change in the amount of RAM according to the show version output

Explanation: While analyzing historical reports an administrator can compare host-to-host timers from the **ping** command and depict possible latency issues.

Question 23

Refer to the exhibit. Host H3 is having trouble communicating with host H1. The network administrator suspects a problem exists with the H3 workstation and wants to prove that there is no problem with the R2 configuration. What tool could the network administrator use on router R2 to prove that communication exists to host H1 from the interface on R2, which is the interface that H3 uses when communicating with remote networks?



- traceroute
- show cdp neighbors
- Telnet
- **an extended ping**

Explanation: An extended ping allows an administrator to select specific ping features. For example in this situation, the network administrator could do an extended ping and specify a source address of the gigabit Ethernet port on the router. The destination address would be the IP address of host H1. If the ping succeeds connectivity exists from the Ethernet router interface on R2 to device H1.

Question 24

Which command can an administrator execute to determine what interface a router will use to reach remote networks?

- show arp
- show interfaces
- **show ip route**
- show protocols

Explanation: The **show ip route** command is used to display the IP routing table of the router. The IP routing table will show a list of known local and remote networks and the interfaces that the router will use to reach those networks.

Question 25

A network technician issues the C:\> tracert - 6 <http://www.cisco.com> command on a Windows PC. What is the purpose of the -6 command option?

- **It forces the trace to use IPv6.**
- It limits the trace to only 6 hops.
- It sets a 6 milliseconds timeout for each replay.
- It sends 6 probes within each TTL time period.

Explanation: The -6 option in the command C:\> tracert - 6 <http://www.cisco.com> is used to force the trace to use IPv6.

Question 26

A ping fails when performed from router R1 to directly connected router R2. The network administrator then proceeds to issue the show cdp neighbors command. Why would the network administrator issue this command if the ping failed between the two routers?

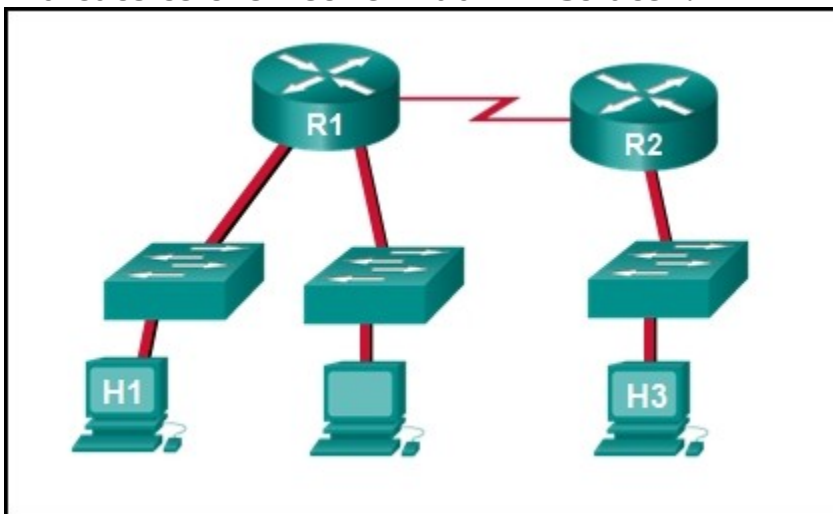
- The network administrator suspects a virus because the ping command did not work.
- **The network administrator wants to verify Layer 2 connectivity.**
- The network administrator wants to verify the IP address configured on router R2.
- The network administrator wants to determine if connectivity can be established from a non-directly connected network.

Explanation: The **show cdp neighbors** command can be used to prove that Layer 1 and Layer 2 connectivity exists between two Cisco

devices. For example, if two devices have duplicate IP addresses, a ping between the devices will fail, but the output of **show cdp neighbors** will be successful. The **show cdp neighbors detail** could be used to verify the IP address of the directly connected device in case the same IP address is assigned to the two routers.

Question 27

Refer to the exhibit. Baseline documentation for a small company had ping round trip time statistics of 36/97/132 between hosts H1 and H3. Today the network administrator checked connectivity by pinging between hosts H1 and H3 that resulted in a round trip time of 1458/2390/6066. What does this indicate to the network administrator?



- Connectivity between H1 and H3 is fine.
- H3 is not connected properly to the network.
- Something is causing interference between H1 and R1.
- Performance between the networks is within expected parameters.
- **Something is causing a time delay between the networks.**

Explanation: Ping round trip time statistics are shown in milliseconds. The larger the number the more delay. A baseline is critical in times of slow performance. By looking at the documentation for the performance when the network is performing fine and comparing it to information when there is a problem, a network administrator can resolve problems faster.

Question 28

A technician is to document the current configurations of all network devices in a college, including those in off-site buildings. Which protocol would be best to use to securely access the network devices?

- FTP
- HTTP
- **SSH**
- Telnet

Explanation: Telnet sends passwords and other information in clear text, while SSH encrypts its data. FTP and HTTP do not provide remote device access for configuration purposes.

Question 29

On which two interfaces or ports can security be improved by configuring executive timeouts? (Choose two.)

- Fast Ethernet interfaces
- **console ports**
- serial interfaces
- **vty ports**
- loopback interfaces

Explanation: Executive timeouts allow the Cisco device to automatically disconnect users after they have been idle for the specified time. **Console**, **vty**, and **aux** ports can be configured with executive timeouts.

Question 30

What is considered the most effective way to mitigate a worm attack?

- Change system passwords every 30 days.
- Ensure that all systems have the most current virus definitions.
- Ensure that AAA is configured in the network.
- **Download security updates from the operating system vendor and patch all vulnerable systems.**

Explanation: Because worms take advantage of vulnerabilities in the system itself, the most effective way to mitigate worm attacks is to download security updates from the operating system vendor and patch all vulnerable systems.

Question 31

Which statement describes the ping and traceroute commands?

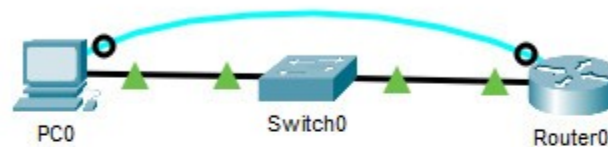
- Ping shows whether the transmission is successful; traceroute does not.
- **Traceroute shows each hop, while ping shows a destination reply only.**
- Both ping and traceroute can show results in a graphical display.
- Traceroute uses IP addresses; ping does not.

Explanation: The **ping** utility tests end-to-end connectivity between the two hosts. However, if the message does not reach the destination, there is no way to determine where the problem is located. On the other hand, the **traceroute** utility (**tracert** in Windows) traces the route a message takes from its source to the destination. **Traceroute** displays each hop along the way and the time it takes for the message to get to that network and back.

Question 32

[Download PT Activity](#)

Open the PT Activity. Perform the tasks in the activity instructions and then answer the question. Which command has to be configured on the router to complete the SSH configuration?



PT Activity: 00:00:49

Use the Terminal application from the Desktop tab on PC0 to access Router0. Note that all passwords are configured as **cisco**. Determine the current partial SSH configuration on Router0.

Which command has to be configured on the router to complete the SSH configuration?

- service password-encryption

- **transport input ssh**
- enable secret class
- ip domain-name cisco.com

Explanation: The missing command to complete the SSH configuration is **transport input ssh** in **line vty 0 4** mode. The commands **service password-encryption** and **enable secret class** do configure secure features on the router, but are not required to configure SSH. The command **ip domain-name cisco.com** is not required because the command **ip domain-name span.com** has been used.

Question 33

When configuring SSH on a router to implement secure network management, a network engineer has issued the **login local** and **transport input ssh line vty** commands. What three additional configuration actions have to be performed to complete the SSH configuration? (Choose three.)

- Set the user privilege levels.
- **Generate the asymmetric RSA keys.**
- **Configure the correct IP domain name.**
- Configure role-based CLI access.
- **Create a valid local username and password database.**
- Manually enable SSH after the RSA keys are generated.

Explanation: SSH is automatically enabled after the RSA keys are generated. Setting user privilege levels and configuring role-based CLI access are good security practices but are not a requirement of implementing SSH.

Question 34

An administrator decides to use “admin” as the password on a newly installed router. Which statement applies to the password choice?

- **It is weak because it is often the default password on new devices.**
- It is strong because it uses a passphrase.
- It is strong because it uses a minimum of 10 numbers, letters and special characters.

- It is strong because it contains 10 numbers and special characters.

Question 35

A network technician is troubleshooting an issue and needs to verify all of the IPv6 interface addresses on a router. What is the best command to use to accomplish the task?

- **show ipv6 interface**
- show interfaces
- show ip nat translations
- show ip route

100%

You have scored **100%**.

Congratulations, you have passed the exam.

You have used 1 of 1 attempt(s).

Review Assessment

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.

Network Basics. Connectivity. Network
100%

Network Basics. Connectivity. Utilities
100%

Security. Security Fundamentals. Hardening
100%